(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23785 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/GB01/04150

(22) International Filing Date:
17 September 2001 (17.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0022724.9 15 September 2000 (15.09.2000) GB

(71) Applicant *(for all designated States except US)*: **INNOVATION VENTURE LIMITED** [GB/GB]; 1st Floor, Exchange House, 54/58 Athol Street, Douglas, Isle of Man IM1 1JD (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **WRIGHT, Michael, Henry** [ZA/ZA]; 1 Scott Street, Waverley, Rutherford Estate, Block B, Johannesburg (ZA). **RAMAGE, Nicholas, Hunter** [ZA/ZA]; 1 Scott Street, Waverley, Rutherford Estate, Block B, Johannesburg (ZA).

(74) Agents: **WRIGHT, Howard, Hugh, Burnby** et al.; Withers & Rogers, Golding House, 2 Hays Lane, London SE1 2HW (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/23785 A2

(54) Title: SECURE MESSAGING

(57) Abstract: A method of secure messaging which includes sending a decoder to a user as an attachment to an e-mail message. The decoder may be sent in the form of an executable file which is installed on a user's computer when the attachment is opened in the e-mail message.

Secure Messaging

Field of the Invention

This invention relates to secure messaging over a communications network.

Background to the Invention

The rapid growth of the Internet has led to widespread use of e-mail as a means of messaging. E-mail is attractive as it is quick and fairly cheap to use. As with transmissions on most communications networks, e-mail does suffer the disadvantage that it can be fairly easily intercepted. For this reason it is often desirable to encrypt messages. Presently, secure messaging is usually performed using a digital certificate and public key encryption. While this can be fairly effective, it is a cumbersome system as digital certificates are often difficult to install and understand, from an end-user perspective, and usually need annual revision. In addition, Public Key Infrastructure and digital certificate solutions require complex certificate management systems and rules. As a result, the system does not lend itself to widespread use.

Systems that do not employ digital certificates still require some form of a decoder, which decrypts messages, to be present on the recipient's computer. At present this entails purchasing proprietary software with a decoder from a vendor and installing it on a computer or downloading a commonly available decoder through a communications network, usually the Internet. The latter is often preferred but can be time-consuming and installation of the decoder difficult. Only once the decoder is installed on a computer can the user sign up to receive encrypted information and this can only be received after the sign up procedure has been successfully completed. The procedure required is thus often too laborious for novices to undertake. In addition, the commonly available solutions have known "cracks" that are also commonly available on the Internet. These cracks are pieces of software that allow one to break the encryption and decipher the information contained therein.

It is particularly desirable to send invoices or statements electronically to clients provided that the information contained therein is only available to authorised users. In this specification "invoice" shall have its widest meaning and shall include statements and accounts unless otherwise indicated.

Also in this specification, "processor" is to be given its widest meaning and includes any suitable apparatus which executes under stored programme control to achieve a desired result.

Object of the Invention

It is an object of this invention to provide secure messaging which will at least partially alleviate some of the above mentioned problems.

Summary of the Invention

In accordance with the invention there is provided a method of secure messaging which includes sending a decoder to a user as an attachment to an e-mail message.

Further features of the invention provide for the decoder to be sent in the form of an executable file; for the decoder to be installed on a user's computer when the attachment is opened in the e-mail message; alternately for the decoder to be installed on a user's computer when the e-mail message is opened.

Further features of the invention provide for the decoder to operatively decrypt encoded information using a key known to the user and to the sender of the information; for the key to be a SHA-1 or MD5 hash of at least two character strings; and for the at least two character strings to include a username and password.

Further features of the invention provide for the encoded information to be sent to a user as an attachment to an e-mail message; for the e-mail message to which the encoded information is attached to also have a decoder attached thereto; for the attachment to invoke the decoder when opened; and for the encoded information to be compressed before being attached to an e-mail message.

A further feature of the invention provides for the information to be encoded using CBC encoded Blowfish or triple DES ciphers.

The invention also provides a method of securely transmitting an invoice which includes encoding the information forming the invoice and transmitting the encoded information to a user as an attachment to an e-mail message and transmitting a decoder for the encoded information to a user as an attachment to an e-mail message.

Further features of the invention provide for the encoded information and decoder to be attached to the same e-mail message; for the decoder to install itself on the user's computer when the e-mail message is opened; alternately for the decoder to install itself on the user's computer when the attachment is opened in the e-mail message.

Further features of the invention provide for the installed decoder to decrypt the encoded information attached to the e-mail message; for the installed decoder to decrypt the encoded information attached to the e-mail message when the attachment is opened; for the decoder to require a key from the user to decrypt the encoded information; and for the key to be known to the user and to the sender of the invoice.

A further feature of the invention provides for the information forming the invoice to be compressed prior to being encoded.

The invention further provides for a system for secure messaging comprising a first store of information and at least one processor configured to encode the information and to attach the encoded information to at least one e-mail message to be sent to at least one user and to attach a decoder to an e-mail message to be sent to the or each user.

Further features of the invention provide for the processor to attach encoded information and a decoder to a single e-mail message to the or each user; for the system to include a mail server for sending the or each e-mail message; for the or each decoder to be an executable file; and for the or each decoder to install itself on a user's computer.

Still further features of the invention provide for the or each decoder to install itself on a user's computer when the attachment is opened in the e-mail message; alternately for the or each decoder to install itself on a user's computer when the e-mail message is opened.

Yet further features of the invention provide for the or each decoder to operatively decode the information attached to an e-mail message using a key known to the user and to the sender of the information; for each key to be a SHA-1 or MD5 hash of character strings; and for the character strings to include a username and password.

Further features of the invention provide for the at least one processor to compress the information prior to encoding it; for the first store of information to include a plurality of sets of information; for each set of information to correspond to a user; and for each set of information to be encoded and attached to an e-mail message.

Still further features of the invention provide for there to be provided a second store of information containing user address details and for a processor to be configured to correlate user details contained in the first information store with those in the second information store and to format e-mail messages using the information in the second store.

Yet further features of the invention provide for the second store of information to further include a username and password for each user; for the processor to encode the information for a user using the username and password for the user contained in the second store of information; and for the or each decoder not to be installed on a user's computer if an identical decoder is already installed on the computer.

A further feature of the invention provide for the at least one processor to interrogate a third store of information in which are recorded details of users who have already received a decoder and wherein the at least one processor does not attach a decoder to an e-mail message to a user where the user is recorded as having already received a decoder.

Brief Description of the Drawings

One embodiment of the invention will be described, by way of example only, with reference to Figure 1 which is a schematic diagram of a secure messaging system.

Detailed Description of the Drawings

A system (1) for secure messaging from a sender (2), in this embodiment a bank, to a plurality of users (20), in this embodiment clients (only one shown), is shown in Figure 1.

Confidential information, for example monthly account statements, generated by the bank's computer system (4) is produced as individual files, or a single file and is stored in a first information store (5) together with necessary identification and addressing information. The files stored at (5) are then sent to a secure server (8) using a secure file transfer protocol (9).

Once received by the secure server (8) through a file data interface (11) the files are parsed (13) into a format understood by the secure server. Hereafter the information in the files is formatted (14) to produce documents of a required type, such as HTML or Word. Once the documents are created, a processor compresses the documents and then encodes the information (15) using a CBC encoded block cipher. The encrypted document is padded with random data for more entropy and to reduce the likelihood of know-plaintext attacks. The process may use any block cipher and key length but in this embodiment supports 112 bit and 168 bit Triple DES or 128 bit to 448 bit Blowfish block ciphers. The key for the encryption is created from a SHA-1 or MD5 hash of the recipient's username and password, which is included in the data files (4). Any suitable character strings may however be used to form the key.

Each encoded file is then attached by the processor to an e-mail message (16) addressed to the relevant user (20) together with a decoder. Each decoder is a small executable file that is capable of decrypting encoded files once properly installed on a computer. Each decoder is further configured to be capable of being installed on a number of different software platforms. This avoids the problem of having to first determine the type of software platform being used by each user (20) and then sending a specific, and

often different, decoder to each user (20). The messages together with attachments are then sent via a bulk mailer (17) using Simple Mail Transfer Protocol (SMTP) to the users (20). Bounced mail (19) will be returned to the mail server (8) for reporting purposes.

Once the e-mail message is received by a user (20), opening the message and executing the decoder (21) will cause the decoder attached to the message to automatically install itself on the user's computer if the user (20) does not already have a decoder. The decoder could, however, also be configured to install automatically when the message is opened. As the size of the decoder is very small, about 43 kb in this embodiment, it is easy to send as an e-mail attachment and simple to manage by the user's computer. Once the decoder is installed on the user's computer all encoded files attached to e-mail messages by the sender (2) will automatically invoke the decoder when they are opened (22). At this point, the user will be required to enter his username and password, which will be used to decode the message (24). If the username/password combination is correct the document is opened using the default viewer (25) for the documents, for example Word or Excel.

The system (1) enables secure messaging to occur through a simple yet highly effective process. By attaching the decoder to an e-mail message it is unnecessary for the user to obtain a decoder by downloading from a communication network or any other means. As the decoder is self installing it is not necessary for the user to have any technical knowledge. Also, the size of the decoder does not impose a large overhead on the e-mail size in terms of bandwidth usage.

It will be appreciated, however, that many other embodiments of a secure messaging system exist especially as regards the configuration thereof and the form of decoder. For example, any suitable encoding can be used and the decoder need not be self-installing and could be installed through any convenient means. The decoder could further be created prior to attachment to a message to decrypt information using a specific key thus obviating the need for the user to enter his password and username for each message. For security reasons, where such a decoder is used, it is desirable for the decoder to require these details prior to installing itself. Alternatively, the decoder could be configured to remember a username and password after they have been entered

once. The decoder could also be attached to a separate message to the message that the encoded information is attached to.

Furthermore, it may be desirable to have two or more stores of information, a first store containing sets information to be encoded together with an identifier for each set, and a second store containing the addressing details and username and password for each identifier. In this instance the processor would obtain addressing details and encoding keys for the information in the first store from the second store of information.

A third store of information, which could form part of the second store of information, could also be used to record whether a user already has a decoder installed on his computer or at least whether he has been sent one. This information could then be checked prior to sending encoded information with an e-mail message to determine whether it is necessary to attach a decoder to the message. Where a decoder is not attached to a message and the user requires one, for example where another computer is being used which does not have a decoder installed, a hyperlink could be provided to allow the user to access a website (secure or otherwise) to download the decoder. Alternatively a device could be provided on messages to automatically request a decoder to be sent to the user.

It will still further be appreciated that the functions of encoding information, attaching the information to a message, attaching a decoder to the message and sending the message may be performed by one or more processors. Where more than one processor is used the processors may each perform a specific task or may operate in parallel.

Claims

1. A method of secure messaging, which includes sending a decoder to a user as an attachment to an e-mail message.

2. A method of secure messaging as claimed in claim 1 in which the decoder is sent in the form of an executable file.

3. A method of secure messaging as claimed in claim 1 or claim 2 in which the decoder is installed on a user's computer when the attachment is opened in the e-mail message.

4. A method of secure messaging as claimed in claim 1 or claim 2 in which the decoder is installed on a user's computer when the e-mail message is opened.

5. A method of secure messaging as claimed in any one of the preceding claims in which the decoder operatively decrypts encoded information using a key known to the user and to the sender of the information.

6. A method of secure messaging as claimed in claim 5 in which the key is a SHA-1 or MD5 hash of at least two character strings.

7. A method of secure messaging as claimed in claim 6 in which the at least two character strings include a username and password.

8. A method of secure messaging as claimed in any one of the preceding claims in which encoded information is sent to a user as an attachment to an e-mail message.

9. A method of secure messaging as claimed in claim 8 in which the e-mail message to which the encoded information is attached also has a decoder attached thereto.

10. A method of secure messaging as claimed in claim 8 or claim 9 in which the attachment invokes the decoder when opened.

11. A method of secure messaging as claimed in claim 8 or claim 9 in which the encoded information is compressed before being attached to an e-mail message.

12. A method of secure messaging as claimed in any one of claims 5 to 11 in which the information is encoded using CBC encoded Blowfish or triple DES ciphers.

13. A method of securely transmitting an invoice which includes encoding the information forming the invoice and transmitting the encoded information to a user as an attachment to an e-mail message and transmitting a decoder for the encoded information to a user as an attachment to an e-mail message.

14. A method of securely transmitting an invoice as claimed in claim 13 in which the encoded information and decoder are attached to the same e-mail message.

15. A method of securely transmitting an invoice as claimed in claim 13 or claim 14 in which the decoder installs itself on a user's computer when the attachment is opened in the e-mail message.

16. A method of securely transmitting an invoice as claimed in claim 13 or claim 14 in which the decoder installs itself on a user's computer when the e-mail message is opened.

17. A method of securely transmitting an invoice as claimed in claim 15 or claim 16 in which the installed decoder decrypts the encoded information attached to the e-mail message.

18. A method of securely transmitting an invoice as claimed in claim 17 in which the installed decoder decrypts the encoded information attached to the e-mail message when the attachment is opened.

19. A method of securely transmitting an invoice as claimed in claim 17 or claim 18 in which the decoder requires a key from the user to decrypt the encoded information.

20. A method of securely transmitting an invoice as claimed in claim 19 in which the key is known to the user and to the sender of the invoice.

21. A method of securely transmitting an invoice as claimed in any one of claims 13 to 20 in which the information forming the invoice is compressed prior to being encoded.

22. A system for secure messaging comprising a first store of information and at least one processor configured to encode the information and to attach the encoded information to at least one e-mail message to be sent to at least one user and to attach a decoder to an e-mail message to be sent to the or each user.

23. A system for secure messaging as claimed in claim 22 in which the processor attaches encoded information and a decoder to a single e-mail message to the or each user.

24. A system for secure messaging as claimed in claim 22 or claim 23 which includes a mail server for sending the or each e-mail message.

25. A system for secure messaging as claimed in any one of claims 22 to 24 in which the or each decoder is an executable file.

26. A system for secure messaging as claimed in any one of claims 22 to 25 in which the or each decoder installs itself on a user's computer.

27. A system for secure messaging as claimed in claim 26 in which the or each decoder installs itself on a user's computer when the attachment is opened in the e-mail message.

28. A system for secure messaging as claimed in claim 26 in which the or each decoder installs itself on a user's computer when the e-mail message is opened.

29. A system for secure messaging as claimed in any one of claims 22 to 28 in which the or each decoder operatively decodes the information attached to a user's e-mail message using a key known to the user and to the sender of the information.

30. A system for secure messaging as claimed in claim 29 in which a key is a SHA-1 or MD5 hash of character strings.

31. A system for secure messaging as claimed in claim 30 in which the character strings include a username and password.

32. A system for secure messaging as claimed in any one of claims 22 to 31 in which the at least one processor compresses the information prior to encoding it.

33. A system for secure messaging as claimed in any one of claims 22 to 32 in which the first store of information includes a plurality of sets of information, each set of information corresponding to a user.

34. A system for secure messaging as claimed in claim 33 in which each set of information is encoded and attached to an e-mail message.

35. A system for secure messaging as claimed in claim 33 or claim 34 in which there is provided a second store of information containing user address details and wherein a processor is configured to correlate user details contained in the first

information store with those in the second information store and to format e-mail messages using the information in the second store.

36. A system for secure messaging as claimed in claim 35 in which the second store of information further includes a username and password for each user.

37. A system for secure messaging as claimed in claim 36 in which the first processor encodes the information for a user using the username and password contained in the second store of information for the user.

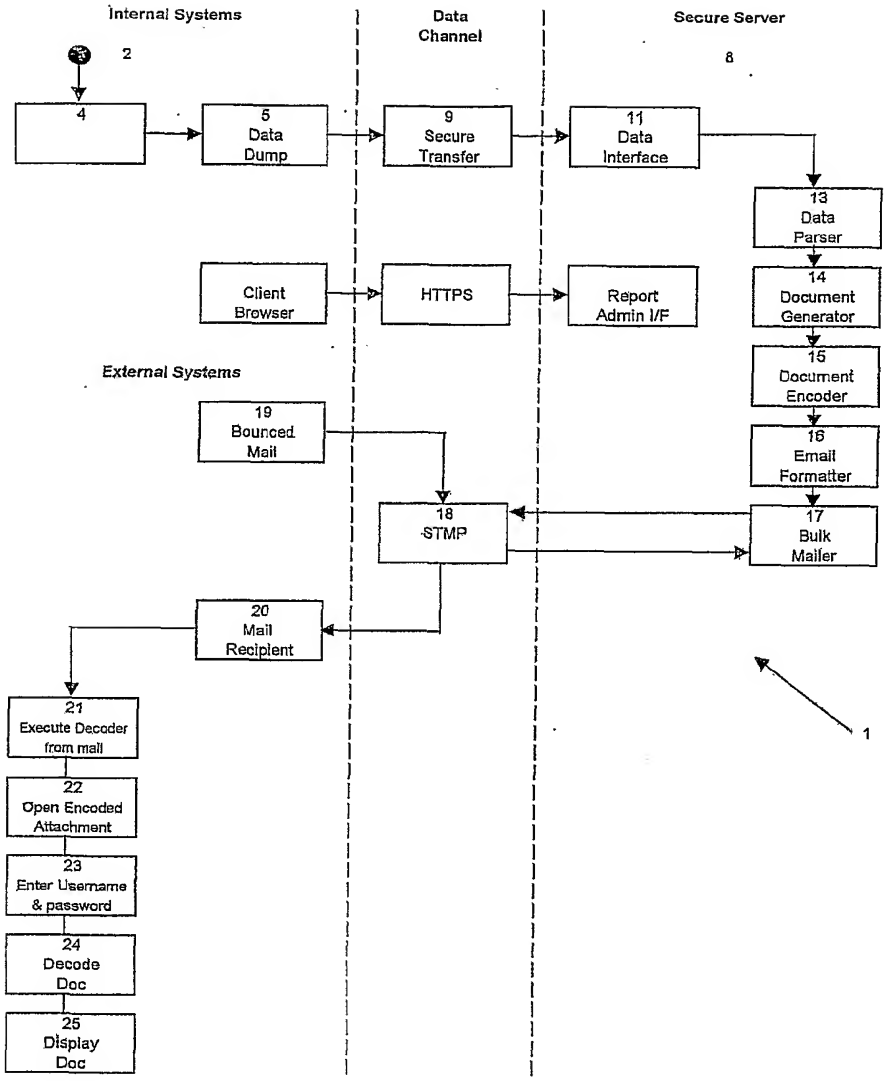
38. A system for secure messaging as claimed in any one of claims 22 to 37 in which the or each decoder is not installed on a user's computer if an identical decoder is already installed on the computer.

39. A system for secure messaging as claimed in any one of claims 22 to 38 in which a processor interrogates a third store of information in which are recorded details of users who have already received a decoder and wherein the at least one processor does not attach a decoder to an e-mail message to a user where the user is recorded as having already received a decoder.

40. A method of secure messaging substantially as herein described and as illustrated with reference to the drawing.

41. A method of securely transmitting an invoice substantially as herein described and as illustrated with reference to the drawing.

42. A system for secure messaging substantially as herein described and as illustrated with reference to the drawing.


Internal Systems
Data Channel
Secure Server
2
8
4
5 Data Dump
9 Secure Transfer
11 Data Interface
13 Data Parser
Client Browser
HTTPS
Report Admin I/F
14 Document Generator
15 Document Encoder
External Systems
19 Bounced Mail
16 Email Formatter
18 STMP
17 Bulk Mailer
20 Mail Recipient
1
21 Execute Decoder from mail
22 Open Encoded Attachment
23 Enter Username & password
24 Decode Doc
25 Display Doc